REMARKS

This amendment is submitted in response to the Examiner's Action dated May 13, 2004. Applicants have amended the claims to clarify key features of the invention and overcome the claim objections and rejections. No new matter has been added, and the amendments place the claims in better condition for allowance. Applicants respectfully request entry of the amendments to the claims. The discussion/arguments provided below in response to the claim rejections reference the claims in their amended form.

IN THE SPECIFICATION/ABSTRACT

In the present Office Action, the abstract of the disclosure is objected to because the total number of words exceeds 150 words. Accordingly, Applicants has amended the abstract to reduce the word count to below 150 words. Applicants respectfully request entry of the amendments to the abstract and removal of the objection.

CLAIMS REJECTIONS UNDER 35 U.S.C. § 112

At paragraph 3 of the Office Action, Claims 5, 13 and 20 are rejected under 35 U.S.C. § 112, first paragraph. Claims 6, 7, 8, 14, 15, 16, 21, 22 and 23 are rejected by virtue of dependency on Claims 5, 13 and 20. Also, at paragraph 5 of the present Office Action, Claims 5-8, 13-16 and 20-23 are rejected under 35 U.S.C. §112 second paragraph, as being indefinite. Applicants have amended the claims to correct the above stated indefiniteness and overcome the § 112 rejections. Applicants, therefore, respectfully request reconsideration and removal of the § 112 rejections.

CLAIMS REJECTIONS UNDER 35 U.S.C. § 102

At paragraph 8 of the present Office Action, Claims 1-7, 9-15, 17-22 and 24-27 are rejected under 35 U.S.C. § 102(e) as being anticipated by *Kern* (U.S. Patent No. 6,336,187 B1). *Kern* does not anticipate Applicants' claimed invention because *Kern* does not teach each feature recited by Applicants' claims.

Applicants' invention provides a hardware-level access security password for storage devices. A security code is programmed into the actual hardware device and is referenced by the

operating system (OS) of a user computer system whenever access to the particular storage device is requested by a user. The user provides a user code for use during executing user-initiated processes (page 11, line 28-31). The user initiated process(es) requests read/write access to the storage device. The OS first retrieves the security code from the storage device and then compares the user-provided user code with the security code (page 12, lines 7-24). The OS permits the process to access the storage device only when the user-provided code matches the security code (page 13, line 21-page 14, line 4).

In one embodiment, the security code is stored in specific bits of microcode on the storage device (page 8, lines 28-page 9, line 1; page 10, line 32- page 11, line 3; etal.). Also, a special OS extension is provided that completes the hardware-level security code retrieval then OS-level user code authentication. This process is distinguishable from the traditional OS-level security methods of checking a user authorization (login and password) to access a computer device (see page 10, ll 15-32).

Applicants' independent claims recite the following features:

(1) "providing a **device-stored hardware-level security code** for a storage device...;" and

(2) "providing within an **operating system (OS)** of a **user computer** an **OS-extension** that enables (1) retrieval of said security code **from** said storage device **to said user computer** system and (2) blocking access to said storage device by **processes on said user computer** system ...; wherein the OS-extension enables use of the **hardware-level security code within a localized, OS-level security checking process,** ...; and allowing access ... only when ...the **localized, OS-level security checking process** to match said hardware-level security code" (emphases added).

Clearly, the concept of a hardware-level security code stored on the storage device itself being utilized by a localized OS-level security check feature on a user (host) computer to determine if to provide access to the storage device is a prominent feature of Applicants' claimed invention. *Kern* is devoid of any teaching or suggestion of this feature recited by Applicant's claims.

Kern generally provides a "host-independent storage facility" that "provides data-dependent security by initially storing a security key in ... a reference location associated with the identified storage region" (Abstract). Specifically, *Kern* stores the security key in a reference location within a **controller**, such as an "IBM RAMAC controller" that is a **separate device, external to the various host devices** and which operates to provide a gating function for granting access to the storage facility (see col. 5, lines 2-17). Beginning at col. 3, line 61 and continuing throughout the patent, *Kern* states that the "host-independent storage controller" is responsible for providing security for the storage regions (col.3, lines 63-65) and to which multiple hosts are connected (col. 4, lines 6-11). The "hosts" represents the user computer systems and range from "personal computers, mainframe computers, ... supercomputers, and other suitable machines" (col. 4, lines 29-32).

At col. 4, lines 51, *Kern* states that "the controller ...operates as a gate...by implementing a data security scheme." At line 57, *Kern* continues that "[s]ince this scheme is **implemented by the controller** 106 **rather than** one or more **hosts** 102-104..." (emphasis added). Following, *Kern* states that "the controller's centrality and independence from the hosts 102-104 ...hosts of many different operating systems."

It is clear from the above cited passages that *Kern* actually teaches a hardware implemented security process, where the security checks for access to the storage device actually takes place on a separate hardware device (controller), which is separate from the user computer on which the access request is provided. This hardware device is not synonymous with nor suggestive of a software OS-extension within the user (host) computer that retrieves the security code of the storage device at the time of an access request by one of the processes executing ont eh user computer.

Further, the use of an OS-extension within a user computer enables the security features of the invention to be applied at a process level within a single computer system (rather than a host computer level within a lager "network type" system). Notably, this deficiency in *Kern* necessarily overcomes any assertions that *Kern* teaches issuing the security code to the OS -

extension of the user computer and any of the related functional features of Applicants' claimed invention.

The standard for a § 102 rejection requires that the reference teach each element recited in the claims set forth within the invention. As clearly outlined above, *Kern* fails to meet this standard and therefore does not anticipate Applicants' invention.

CLAIM REJECTIONS UNDER 35 U.S.C. § 103

At paragraph 23 of the present Office Action, Claims 8, 16 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Kern* in view of *Wu* (U.S. Patent No. 5,774,551). These claims all depend from respective independent claims, which Applicant have shown to be allowable. Thus, the present claims are also rendered allowable.

Notably, however, Applicants point out that Examiner incorrectly attributes to *Wu* a teaching of restricting subsequent access to the storage device when the security code does not match the user code during the first request. Examiner cites to col. 14, lines 4-11 of *Wu*, which describes completing a number of authentication attempts up to a predetermined maximum number. One skilled in the art would not find this known method of checking when a predetermined number of attempts to enter security information (passwords, etc.) is exceeded to read on or be suggestive of automatically restricting access to a storage device when a first process attempting access to the device fails.

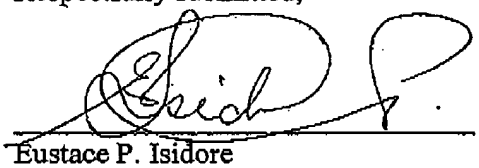
Given the above reasons, it is clear that the combination of references does not suggest the above features of Applicants' dependent claims. The above claims are therefore allowable over the combination.

CONCLUSION

Applicants have diligently responded to the Office Action by amending the Abstract to overcome an objection thereto. Applicants have also amended the claims to clarify certain features of the invention and overcome the § 112, § 102 and § 103 rejections. The amendments along with the accompanying arguments overcome the claim rejections, and Applicants, therefore, respectfully request issuance of a Notice of Allowance for all claims now pending.

Applicants also request the Examiner contact the undersigned attorney of record at 512.343.6116 if such would further or expedite the prosecution of the present Application.

Respectfully submitted,



Eustace P. Isidore
Registered with Limited Recognition (see attached)
Dillon & Yudell LLP
8911 North Capital of Texas Highway
Suite 2110
Austin, Texas 78759
512.343.6116

ATTORNEY FOR APPLICANT(S)